NISD-K304-111

Common Standards for Information Security Measures for The Government Agencies

May 19, 2014

Established by the Information Security Policy Council

Table of contents

Chapter 1 General Provisions

1.1 Purpose and Scope of these Common Standards for Measures

(1) Purpose of these Standards

The basic principal of information security is to ensure “confidentiality”, “integrity”, and “availability” of the information handled by government agencies according to the degree of importance of information, and it is a fundamental responsibility for each government agency to duly implement measures to ensure information security. However, under the current circumstances where the government agencies use and share the common IT environment as well as information, it is necessary to formulate a unified framework to raise the level of information security standards across the agencies.

These Common Standards set forth the measures that the government agencies should implement to ensure and further enhance information security within the unified framework in accordance with the “Common Rules of Information Security Measures for Government Agencies “(established by the Information Security Council on May 19, 2014).

(2) Scope of these Standards

(a) These Standards shall apply to all employees engaged in administrative services at government agencies.

(b) These Standards shall apply to the information defined below:

(i) Information used by employees to perform their duties, which is recorded on the information systems procured or developed by government agencies, or information recorded on the external storage media (including information printed out from, or input in the system).

(ii) Information for use of employees, recorded on other information systems or other external storage media (including the information printed out from, or input in the system).

(iii) In addition to (i) and (ii), information concerning the design or operational management of the system procured or developed by government agencies.

(c) These Standards shall apply to all information systems which process the information stipulated herein.

(3) Revisions of these Standards

It is important to precisely understand changes in circumstances and accordingly review information security measures to maintain an appropriate level of information security. Therefore, these Standards shall be regularly reviewed and necessary additions and amendments shall be made according to information technology development.

(4) Compliance with laws and regulations

When taking information security measures, laws and regulations which stipulate handling of information and information systems (hereinafter referred to as “relevant laws and regulations”)

should be respected in addition to these standards. These Standards provide no reference to such relevant laws and regulations, as they should be respected regardless of information security measures. Equally the government's resolutions set forth in response to changing environment of information security should be duly observed.

(5) Contents of the measures

In these common standards, measures to be implemented by government agencies are classified into 3 layers, namely chapters, sections, and paragraphs according to the purpose, and each paragraph specifies purpose, and compliance requirements. The compliance requirements set forth the measures mandatory to implement the standards for measures for government agencies. When formulating standards for measures, reference should be made to the Guidelines for Establishing Standards of Measures for Government Agencies, established by the National Information Security Center, as well as prerequisites, examples, and comments for measures' implementation, which conform to the compliance requirements stipulated in application manuals of Common Standards for Measures.

1.2 Classification of Information and Handling Restrictions

(1) Classification of information

These Standards classify information in three aspects namely confidentiality, integrity, and availability, whose definition are shown below. When changing or adding classifications, each government agency shall ensure the relationships between classifications and requirements for given measures to be the same or higher than those described in these Standards. The government agency should appropriately notify the classifications set forth in the Standards, as well as its own corresponding classification, when providing information to other government agencies.

Classifications for confidentiality

Classification	Classification criteria
Confidentiality class-3 information	Among information for administrative use, items which are considered confidential and required to be handled accordingly.
Confidentiality class-2 information	Among information for administrative use, items, though not considered confidential, whose leakage may infringe citizens' rights or hamper the administrative operations.
Confidentiality class-1 information	Information other than Confidentiality class-2 information or Confidentiality class-3 information, such as information disclosed or can be disclosed.

Information which comes under Confidentiality class-2 information and Confidentiality class-3 information is called “confidential information”.

Classifications for integrity

Classification	Classification criteria
Integrity class-2 information	Among information for administrative use (except for written information), items whose manipulation, errors, and damage may infringe citizens' rights or hamper proper administrative operations (except for negligible cases).
Integrity class-1 information	Information other than Integrity class-2 information (except for written information)

Note that Integrity class-2 is called “critical information”.

Classification for availability

Classification	Classification criteria
Availability class-2 information	Among information for administrative use (except for written information), items whose disappearance, loss, or unavailability may infringe citizens' rights or stable administrative operations (except for negligible cases).
Availability class-1 information	Information other than Integrity class-2 information (except written information.)

Note that Availability class-2 information is called “vital information”.

Also, confidential information, critical information, and vital information are collectively called “classified information”.

(2) Types of handling restrictions

“Handling restrictions” means restrictions to ensure proper handling of information by employees, such as to prohibit copying, removing, and distributing information, as well as mandatory encryption and disposal of the data after use.

The employees should appropriately handle the information according to its classification, and follow the types of handling restrictions to demonstrate proper and practical handling of the information. Government agencies should set forth the basic definitions of handling restrictions from perspectives of three aspects, namely confidentiality, integrity, and availability.

1.3 Definition of Terms

【A】

- “Areas requiring control measures” means areas under the control of government agencies such as government office buildings (including facilities leased from external organizations), where control measures for the facilities and environment are required to protect information.

【C】

- “Communication line” means mechanisms for transmitting and receiving information among several information systems, and also among several equipment (including devices not purchased by government agencies), as well as between information systems and equipment, using prescribed communication protocol. Unless otherwise specified, it is a generic term referring to the communication lines used for information systems at government agencies. Communication line includes the one which is not directly managed by government agencies and also includes all connections regardless of their types (such as wire or wireless, physical or virtual).
- “Communication line equipment” means a device which connects communication lines, as well as communication lines and information systems, and controls information transmitted and received over these lines. Communication line equipment includes hubs, switches, routers, and firewalls.
- “Communication line inside the government agency” means a communication line used for communication between the server equipment and terminals managed by a government agency, which has no logical connection with the server equipment and terminals not being managed by said government agency. Communication line inside the government agency also means those whose physical lines are not managed by government agencies, such as proprietary lines and VPNs.
- “Communication line outside the government agency” means a communication line other than “Communication line inside the government agency”.
- “CSIRT” means a system established at government agencies to respond to information security incidents which occur therein. An acronym for Computer Security Incident Response Team.
- “CYMAT” means a system established in the National Information Security Center which provides proactive support for information security incidents which require unified actions with the government, in the event of, or fear of information security failure at government agencies due to cyber-attacks and so forth. An acronym for Cyber Incident Mobile Assistance Team (information security emergency support team).

【E】

- “Employees” means legal employees such as government officials and those who are under supervision of government agencies, who handle information and information systems managed by government agencies. Employees also include dispatched workers, though it depends on individual work conditions.

- “Equipment, etc.” means a collective term for information systems components (such as servers, terminals, communication line equipment, multiple function devices and other apparatus for specified purposes, and software), as well as external storage media.
- “Equipment for specific purposes” means information system components for specific purposes as in the systems for TV conference, IP phones, and network cameras and so forth, which are connected to communication lines or equipped with external storage media.
- “Erasure” -> See “Information erasure”
- “External services on general terms and conditions” means information processing services by organizations other than government agencies such as private sectors, whose server equipment are used by the users to create, store, and transmit information. Those services which enable users to implement necessary and sufficient setting for information security shall not be in this category.

【G】

- “Government Agencies” collectively refers to organizations stipulated by law and established within or under jurisdiction of the Cabinet, the Imperial Household Agency, organizations stipulated in Article 49 Paragraph (1) or (2) of the Act for Establishment of the Cabinet Office (Act No. 89 of 1999), organizations stipulated in Article 3 Paragraph (2) of the National Government Organization Act (Act No. 120 of 1948), and other organizations which fall under these organizations. “The Government Agency” means a single organization.

【I】

- “Implementation procedures” means practical procedures need to be determined beforehand to implement the measures prescribed in the standards for measures for individual information systems and tasks of government agencies.
- “Information” means the information set forth in 1.1. (2) (b) of these Standards.
- “Information erasure” means to make all the information recorded in external storage media unusable and unrestorable. Erasing information shall mean deletion of information as well as physical destruction of the storage media containing the information. If the information can be recovered by revoking deletion or using a recovery tool, it cannot be referred to as “Information erasure”.
- “Information security rules” is a collective term for all standards for measures and operational procedures implemented by government agencies.
- “Information security incidents” means information security incidents set forth in JIS Q 270001:2006.
- “Information system” means systems consist of hardware and software (including those managed by outsourcing contractors), which are used for information processing and communications, and developed and procured by government agencies unless otherwise specified.

【L】

- “Labeling, etc.” means a measure to make information's classification clear to all who handle the information. This means to display the classification of information and any other actions to make the information classification a common knowledge. One of the examples of such measure

is, to indicate the classifications of information recorded in a specific information system by describing them in regulations, and to make them known to all the users of said system.

【M】

- “Malware” (a short form for malicious programs or software) means software in general which causes unsolicited results to information systems such as computer viruses, worms (not parasitic but self-replicating program), and spywares (program which collects various information against users’ will).
- “Mobile terminal” means, regardless of its type, a terminal designed to be carried around according to users’ business needs.

【O】

- “Outsourcing party” means an external contractor undertakes part of, or all of information processing tasks for government agencies.
- “Outsourcing” means contracting out part of, or all of information processing tasks of government agencies, including all types of contracts such as “mandate”, “quasi-mandate”, or “contract”.

【S】

- “Server equipment” means the components of information system which provide own services to terminals and other devices getting access to it via communication lines and other means (including components such as pre-loaded software, built-in mouse and keyboard), and unless otherwise specified those procured or developed by government agencies.
- “Standards for measures for government agency” means standards for information security measures to ensure information security of information and systems at government agencies.
- “Storage media” means media in which information is recorded or written. Storage media includes written document, and any paper or other tangible objects on which human-recognizable information such as characters or diagrams are written (hereinafter referred to as “hardcopies”), and those on which information unrecognizable by human is recorded electronically or magnetically, and are processed by computers (hereinafter referred to as “electromagnetic data”, “external storage media”, respectively). The external storage media can be internal storage media built into server equipment, terminals, and communication equipment, or external storage media such as USB memories, external HDDs, and DVD-Rs.

【T】

- “Terminal” means the equipment of information system component which an employee directly operates (including the operating system and connected peripheral devices such as keyboard and mouse), and unless otherwise specified those procured or developed by government agencies. “Terminal” also means mobile terminals.

Chapter 2 Basic Framework of Information Security

2.1 Introduction and Plan

2.1.1 Establishment of organizations and systems

Purpose

Implementation of information security measures can be accomplished when employees therein fully understand the authority and responsibilities related to their job positions and functions, and duly fulfil those responsibilities. To achieve this it is essential to clearly define such authority and responsibilities and establish necessary organizations and systems. In particular, the chief information security officer should direct and encourage the entire organization to systematically execute measures to ensure a steady promotion of information security measures.

The chief security officer can delegate part of his authority to officers in charge set forth in this Standards.

Compliance Requirements

(1) Designation of the chief information security officer
   (a) The chief information security officer shall be designated to direct tasks associated with information security measures at government agencies.

(2) Establishment of the Information Security Committee
   (a) The chief information security officer shall establish the Information Security Committee, which consists of representatives of departments promoting information security and of other departments engaged in administrative tasks, whose function is to deliberate provisions such as the standards for measures for government agencies.

(3) Designation of the chief information security auditor
   (a) The chief information security officer shall designate the head information security auditor who directs tasks associated with audits conducted under the direction of the chief information security officer.

(4) Designation of the head information security officer and information security officers
   (a) The chief information security officer shall designate an information security officer who directs tasks of information security measures for each unit of organization where the same quality of such measures can be implemented. One of the information security officers shall be designated by the chief information security officer as the head information security officer, who directs all information security officers and assists the chief information security officer.
   (b) Information security officers shall designate an area information security officer who directs tasks of information security measures for each area set forth in the compliance requirements 3.2.1(2)(a).
   (c) Information security officers shall designate a division/office information security officer for each office who directs information security related work.

(d) In the planning phase of such information security, information security officers shall designate information system security officers who are responsible for tasks concerning information security measures in the divisions under their management.

(5) Designation of the chief information security advisor

(a) The chief information security officer shall designate the chief information security advisor with expertise and experience in information security, and define the job descriptions of the position including advisory functions for the chief information security officer.

(6) Establishment of the system for information security incidents

(a) The chief information security officer shall manage and clarify the role of CSIRT.

(b) The chief information security officer shall designate employees deemed to have expertise and competence in information security as officers in charge of CSIRT. One of the CSIRT officers shall be designated as the head CSIRT officer who directs measures in the event of information security incident at government agencies.

(c) The chief information security officer shall establish a reporting system through which all concerning parties immediately report to him or her in the event of security information incident.

(d) The chief information security officer shall designate employees who are in charge of CYMAT.

(7) The roles that should not be concurrently undertaken by the same person

(a) Employees shall not concurrently undertake the following roles when implementing information security measures.

(i) A submitter of an application for approval or permission (hereinafter referred to as “approval, etc.” in this paragraph), and a person who approves the application (hereinafter referred to as “the approval authority, etc.” in this paragraph).

(ii) An auditee and an auditor

(b) When applying for approval, etc., if employees themselves are the approvers, or if it is irrelevant for the approval authority, etc. to decide whether the application should be approved or denied, such approval, etc. should be submitted to, and granted by, their supervisors or other parties deemed relevant.

2.1.2 Establishment of standards for measures and promotion plan for the measures

Purpose

In order to appropriately maintain the level of information security at government agencies and comprehensively reduce information security risks, it is important to establish standards for the measures with which government agencies should comply, and to systematically implement measures based on the risk assessment of information security.

Compliance Requirements

(1) Establishment of the standards for measures for government agencies
   (a) The chief information security officer shall establish the standards for measures for government agencies conforming to the Common Standards for Measures, through deliberation by the Information Security Committee.

(2) Establishment of the measure promotion plan
   (a) The chief information security officer shall establish a plan to comprehensively promote information security measures (hereinafter referred to as the “measure promotion plan”) through deliberation by the Information Security Committee. In addition, the measure promotion plan shall include an overall policy based on the risk assessment results of the tasks and information handled by government agencies, as well as the information systems owned by these government agencies. The plan shall also contain the policies for initiatives, significant points, and the implementation schedules which are indicated below.
      (i) Education on information security
      (ii) Self-assessment of information security measures
      (iii) Information security audit
      (iv) Initiatives to promote technical measures related to information systems
      (v) Any other important initiatives related to information security measures listed in the preceding items

2.2 Operation

2.2.1 Enforcement of information security related provisions

Purpose

It is necessary for government agencies to establish specific operational procedures to implement the measures stipulated in the standards for measures for government agencies.

If the operational procedures for the measures are improperly organized or lack some processes, they may not be duly implemented. Therefore, it is important for the chief information security officer to instruct the head information security officer to maintain operational procedures and receive periodic reports to clearly understand the maintenance status.

Compliance Requirements

(1) Implementation and maintenance of operational procedures for information security measures
   (a) The head information security officer (unless otherwise specified in this Standards) shall maintain the operational procedures for information security measures at government agencies and direct tasks concerning the operational procedures, and report the maintenance status to the chief information security officer.
   (b) The head information security officer shall maintain personnel management rules for information security measures, such as the start and end of employment, and personnel changes.

(c) The information security officers or division/office information security officers shall report to the head information security officer, if there are any issues or problems with information security related provisions reported by employees.

(2) Handling violations
   (a) Employees shall report to the information security officers when they become aware of any serious breach of information security related provisions.
   (b) The information security officers shall instruct the violator and concerned parties to take necessary measures to maintain information security when he or she is informed of, or becomes aware of any serious breach of information security related provisions, and shall report to the chief information security officer through the head information security officer.

2.2.2 Exceptional measures

Purpose

There may be situations where employing methods other than those prescribed, or not implementing the prescribed measures should be approved, due to the reasons such as applying certain information security related provisions shall significantly hinder appropriate execution of administrative tasks. To handle such situations, it is necessary to establish procedures for exceptional measures.

Compliance Requirements

(1) Maintenance of exceptional measures
   (a) The chief information security officer shall designate a person who examines applications for exceptional measures (hereinafter referred to as “the permission authority”) and shall establish the examination procedure.
   (b) The head information security officer shall maintain the records of exceptional measure application and request the permission authority to regularly report on application status.

(2) Operation of exceptional measure
   (a) Employees shall follow the stipulated examination procedures when submitting applications for exceptional measures to the permission authority. In case that a task should be executed immediately and can be handled with utmost respect for provisions, where taking measures other than those prescribed in the information security related provisions or not taking prescribed measures is unavoidable, applications for such exceptional measures shall be promptly submitted afterwards.
   (b) The permission authority shall examine applications for exceptional measures submitted by employees in accordance with the stipulated approval procedures and determine whether or not to approve.
   (c) The permission authority shall establish records of exceptional measure application and report them to the head information security officer.

(d) The head information security officer shall review information security measures for necessary revisions or additions based on the application status of exceptional measures, and report them to the chief information security officer.

2.2.3 Education

Purpose

Even when the information security related provisions are appropriately maintained, the level of information security cannot be enhanced if employees are not informed of, nor comply with their contents. Therefore, it is essential for all employees to acquire deeper knowledge of information security related provisions through education to appropriately implement information security measures.

Compliance Requirements

(1) Maintenance of frameworks of information security measures education
   (a) The head information security officer shall establish education plans on information security measures based on the measures promotion plans, and maintain their enforcement framework.

(2) Enforcement of information security measures education
   (a) The division/office information security officer shall ensure employees to duly participate in information security measure education.
   (b) Employees shall duly participate in information security measure education, according to the education plan.
   (c) The division/office information security officer shall ensure officers in charge of CYMAT and CSIRT to duly participate in information security measure education.
   (d) The head information security officer shall report to the chief information security officer on enforcement status of information security measures education.

2.2.4 Handling of information security incidents

Purpose

If an information security incident is detected, it should be immediately reported to the chief information security officer, and the measures to prevent the spread of damage as well as for recovery, should be implemented. Also, after handling the incident, it is important to identify the lessons to be learned by investigating the root causes, and utilize those lessons to prevent recurrence, and to review the systems and procedures.

Compliance Requirements

(1) Preparation for information security incidents
   (a) The head information security officer shall establish/maintain reporting procedures, including points of contact within the government agencies in the event of information security incidents, and shall inform all employees of these procedures.

(b) The head information security officer shall establish/maintain procedures for measures including sharing information with parties other than government agencies in the event of information security incidents.

(c) In preparation for information security incidents, the head information security officer shall establish an emergency communication network containing emergency contacts, communication methods, and contents to report, for the information systems deemed especially critical to execute administrative tasks.

(d) The head information security officer shall examine the necessity of education on measures against information security incidents, and establish/maintain the contents and framework of the education for the information systems deemed especially critical to execute administrative tasks.

(e) The head information security officers shall establish/maintain points of contact to receive reports on information security incidents from parties other than government agencies, and inform them of the method to communicate with such point of contact.

(2) Reporting and response flow in the event of information security incidents

(a) Employees shall report to the points of contact at government agencies and follow their instruction in the event of information security incidents.

(b) The head CSIRT officer shall verify the circumstances and immediately report to the chief security officer in the event of information security incidents.

(c) The CSIRT shall provide the relevant information security officers concerning the detected information security incident with instructions or advice on emergency measures to prevent spread of damage, or to recover from the incident.

(d) Information security officers shall implement appropriate measures based on procedures stipulated by government agencies, or on CSIRT instructions or advice, in the event of information security incidents against the information security system under their management.

(e) In the event of information security incidents affecting information systems shared by multiple government agencies (excluding such information systems whose entire operations including hardware and software are controlled and managed by a single government agency. Hereinafter referred to as " fundamental information systems"), where the information security provisions for system operation and management of such fundamental information security systems are available, information security officers shall duly follow those provisions when implementing measures.

(f) CSIRT shall immediately report to the National Information Security Center in the event of information security incidents against information security systems at government agencies. In case that the detected information security incidents are cyber-attacks or likewise, CSIRT shall report to the police depending on the contents of such information security incidents. Furthermore for threats such as large scale cyber-attacks which cause or may cause significant damage to the citizen's life, body, property, and national land, CSIRT shall make

a report in accordance with “Initial countermeasures for large-scale cyber-attacks” (March 19, 2010, decided by the Deputy Chief Cabinet Secretary for Crisis Management).

(g) CSIRT shall share the details of information security incidents with concerning bodies, including government agencies.

(h) CSIRT shall provide necessary information to CYMAT when receiving their supports.

(3) Investigation in the event of information security incidents and prevention of recurrence

(a) Information security officers shall, upon receiving instructions from CSIRT, investigate the cause of information security incidents based on such instructions or advice, and review the measures for prevention and report them to the chief information security officer.

(b) The chief information security officer shall examine the report on information security incidents submitted by information security officers, and take necessary measures to prevent recurrence.

2.3 Inspection

2.3.1 Self-assessment of information security measures

Purpose

To ensure effectiveness of information security measures it is vital to assess how the information security related provisions are complied with, and to analyze the results of such assessments.

It is important to appropriately carry out self-assessment to see if an employee duly carries out the measures implemented according to his or her role, and also to assess the level of information security in the entire organization.

In addition, it is important for each concerning party to implement the necessary revised measures within the scope of his or her responsibility for the role, based on the results of self-assessment.

Compliance Requirements

(1) Formulation of self-assessment plans and establishment of procedures

(a) The head information security officer shall formulate an annual plan for self-assessment based on the measures promotion plan.

(b) Information security officers shall maintain self-assessment forms and procedures for each employee.

(2) Conducting self-assessment

(a) Information security officers shall instruct employees to conduct self-assessment in accordance with the annual self-assessment plan.

(b) Employees shall conduct self-assessment using the self-assessment forms and procedures prepared by information security officers.

(3) Evaluations and improvements based on self-assessment

(a) The head information security officer and information security officers shall analyze and evaluate the self-assessment conducted by employees, and report the evaluation results to the chief information security officer.

(b) The chief information security officer shall evaluate the overall results of self-assessment and instruct information security officers to make improvements on any identified issues.

2.3.2 Information security audit

Purpose

To ensure effectiveness of information security measures it is also vital to ensure that an independent party to carry out information security audit, while parties engaged in information security measures to conduct self-assessment.

In addition, it is important for the chief information officer to instruct information security officers to implement necessary measures based on the issues identified by the audit.

Compliance Requirements

(1) Formulation of audit plans

(a) The head information security auditor shall formulate plans for information security audit based on the measure promotion plan.

(b) The head information security auditor shall conduct additional audits that are not defined in the measure promotion plan, in case the chief information security officer instructs to perform such audits to respond to situational changes in information security.

(2) Conducting information security audit

(a) The head information security auditor shall instruct information security auditors to conduct audits in accordance with the measure promotion plan, and provide the chief security officer with an audit report containing the following items.

(i) The audit shall confirm that the matters stipulated in the standards for measures for government agencies are in accordance with the Common Standards for Measures.

(ii) The audit procedures shall be in accordance with the standards for measures for government agencies

(iii) The audit shall confirm if operations in auditees' departments are in accordance with the information security related provisions, by verifying matters such as adequately conducted self-assessments.

(3) Responding to audit results

(a) The chief information security officer shall instruct information security officers to take measures against any issues pointed out in the audit report.

(b) The information security officers shall formulate improvement plans for the issues for which the chief information security officer requests improvements based on the audit report and so on.

2.4 Review

2.4.1 Review of information Security measures

Purpose

As the environment surrounding information security is constantly changing, the level of information security cannot be maintained if these changes are not appropriately addressed. Therefore, it is necessary to conduct periodical reviews on the information security related provisions which serve as the basis for information security measures for government agencies, taking into account the matters such as issues with actual operations, results of self-inspections and audits.

It is also vital to comprehensively evaluate the results of self-inspections and audits and review the initiatives for information security to further promote them.

Compliance Requirements

(1) Review of information security related provisions

(a) The chief information security officer shall comprehensively evaluate the information security operation and the results of self-assessments and audits, and conduct a necessary review on the standards for measures for government agencies, taking into account the significant situational changes in information security, and after deliberations of the Information Security Committee.

(b) The head information security officer shall review the information security operation procedures, taking into account the information security operations and the results of self-assessments and audits, or shall instruct who prepared the procedures to review the provisions, and report the results to the chief information security officer.

(2) Review of measure promotion plan

(a) The chief information security officer shall comprehensively evaluate the information security operation and the results of self-assessments and audits, and conduct a necessary review on the measures promotion plan, taking into account the significant situational changes in information security, and after deliberations of the Information Security Committee.

Chapter 3 Information Handling

3.1 Information Handling

3.1.1 Information handling

Purpose

Execution of administrative tasks requires information handling such as preparation, obtainment, use, storage, provision, transportation, transmission, and deletion (hereinafter referred to as "use or handling" in this section). In order to maintain the security of certain information, all employees who use or handle such information need to implement appropriate measures corresponding to its characteristics at each phase of the information lifecycle.

For this reason, it is necessary for employees to take actions such as labeling classifications and handling restrictions of information upon its preparation or obtainment, to share the same understanding on handling of such information, as well as to implement measures in accordance with its classification and handling restrictions.

Compliance Requirements

(1) Maintenance of provisions related to information handling

(a) The head information security officer shall maintain the provisions of information handling which contains the following items and notify them to employees.

(i) Definitions of "classifications and handling restrictions of information"

(ii) Procedures of labeling, etc. of "classifications and handling restrictions of information"

(iii) Procedures of maintenance and review of "classifications and handling restrictions of information"

(2) Prohibition of use or handling of information for non-job related purposes

(a) Employees shall limit the use or handling of the information within the scope of their job functions.

(3) Determining and labeling, etc. of classifications and handling restrictions of information

(a) When preparing information or start managing information prepared by parties other than government agencies, employees shall determine the classifications and handling restriction of information in accordance with its definitions, and take necessary actions such as labeling them.

(b) When classifying information as confidentiality class-3, employees shall label or clearly indicate the duration for which the given information should be handled under such classification.

(c) When preparing or duplicating information, employees shall maintain the same confidentiality classification and handling restrictions as the original, if the obtained or referred original information is already classified according to its level of confidentiality.

(d) If the existing classifications and handling restrictions deem necessary to be reviewed for amendments, additions, deletions, and for other reasons, employees shall consult with a

person, or his or her senior, who determines the classifications and handling restrictions (including those who follow the determination- hereinafter referred to as the "classifying authority in this section), and conduct reviews based on the outcome of such consultation.

(4) Use and storage of information

(a) Employees shall appropriately handle information in accordance with the classification and handling restrictions, which is labeled, or otherwise specified.

(b) Employees shall obtain permission from their information system security officers and division/office information security officers when processing confidentiality class-3 information outside of the areas requiring control measures.

(c) Employees shall take necessary security management measures when processing classified information outside of the areas requiring control measures.

(d) Employees shall appropriately manage information in accordance with the classification and handling restrictions of information, such as setting access control when saving information.

(e) Employees shall follow the prescribed procedures when handling information using external storage media, such as USB memories and so on.

(5) Provision and disclosure of Information

(a) When disclosing information, employees shall make sure the information is classified as class 1 information.

(b) When providing information to parties outside of the scope of viewing restrictions, employees shall consult with the classifying authority and follow his or her decision. In addition, employees shall ensure that the information is properly handled in accordance with the prescribed classification and handling restrictions at the parties' sites. To achieve this employees shall take measures such as to assuredly inform the parties of points to be noted when handling such information.

(c) Employees shall obtain approval from their division/office information security officers when providing confidentiality class-3 information to parties outside of the scope of viewing restrictions.

(d) When providing or disclosing information in electromagnetic format, employees shall take measures to prevent inadvertent information leakage from supplemental information such as update history and document properties.

(6) Transportation and transmission of information

(a) When transporting confidentiality class-3 information, critical information or vital information to places outside of the areas requiring control measures, or transmitting such information via communication line outside the government agency, employees shall obtain permission from their division/office information security officers.

(b) When transporting an external storage media which stores or contains classified information to places outside the areas requiring control measures, employees shall select the means of transportation with considerations to security and take appropriate measures

to ensure security in accordance with the classification and handling restrictions of the information. In case that the media is transported only to an area pre-designated by the head security officer, where defined as the areas required handling restrictions by other government agencies, such area shall be regarded as an area requiring control measures.

(c) When transmitting classified information in electromagnetic format such as e-mail, employees shall select the means of transmission with considerations to security, and take appropriate measures to ensure security in accordance with the classification and handling restriction of information.

(7) Deletion of information

(a) Employees shall immediately erase the information stored in an external storage media when it becomes unnecessary for their job functions.

(b) When disposing of an external storage media, employees shall erase all the information stored, making it completely unrestorable and ensuring there is no remaining information in the media.

(c) When disposing of confidential information in written format, employees shall make it unrestorable.

(8) Backup of information

(a) Employees shall take backup of information in an appropriate manner in accordance with the classification of information.

(b) Employees shall determine the place, manner, period for storage and so on, of the backup information, and appropriately manage it in accordance with the classification and handling restriction of information.

(c) Employees shall appropriately delete, erase or dispose of the information with exceeded storage period, in accordance with the provisions set forth in paragraph (7) of this section.

3.2 Information Handling Areas

3.2.1 Information handling areas

Purpose

When the server equipment, terminals and other equipment are installed in an environment physically accessible by unspecified large number of publics, there are risks such as malicious impersonation, physical destruction to the equipment, and information leakage caused by illegal removal of such equipment. Other threats concerning the environment where the systems are installed include damage to information systems as a result of disasters.

Therefore, it is necessary to ensure security of information and information systems in the areas including offices, conference rooms, and server rooms where information is handled, by implementing measures such as physical countermeasures, as well as entrance and exit management systems, and so on.

Compliance Requirements

(1) Determine the standards for measures for the areas requiring control measures

(a) The head information security officer shall determine the scope of the areas requiring control measures.

(b) The head information security officer shall determine the standards for measures for the areas requiring control measures according to the characteristics of each area which include the following items.

(i) Physical measures to prevent easy access to the areas by unauthorized persons, including maintenance and installation of facilities such as lockable doors and partitions.

(ii) Entrance and exit management systems to restrict unauthorized persons to enter the areas, as well as to prevent illegal actions by authorized persons while they are in the areas.

(2) Determine the measures to be implemented in each area

(a) Information security officers shall determine areas per unit where they implement measures for facilities and environments based on the standards set forth by the head information officer.

(b) Area information security officers shall determine measures to be implemented in the areas they manage, considering the matters such as the standards set forth by the head information officer, surrounding environment, type of administrative tasks, and information handled in such areas.

(3) Implementation of measures for the areas requiring control measures

(a) Area information security officers shall implement measures determined in the areas they manage. As for the measures need to be carried out by employees, area information security officers shall take actions to ensure that employees duly understand and recognize such measures.

(b) Area information security officers shall implement physical measures to protect information systems which handle vital information from disasters.

(c) Employees shall use the areas in accordance with the measures determined by area information security officers. Employees shall ensure those who belong to parties other than their own government agencies use the areas in accordance with the prescribed measures when allowing such external parties to enter the areas.

Chapter 4 Outsourcing

4.1 Outsourcing

4.1.1 Outsourcing

Purpose

When the development of information systems, application programs, and so on are outsourced to external parties which makes it difficult for employees to directly manage the information security measures at the outsourcing parties, it would be vital to specify requirements for outsourcing parties in documents such as procurement specifications and include them in terms of contracts, in order to ensure the information security measures conforming to the standards for measures for government agencies are duly implemented by outsourcing parties.

There are variety of outsourcing as shown in the examples below, and forms of outsourcing contracts vary from subcontracting, entrustment, to sub-entrustment, and so on. In any case it is important to clearly define the scope of outsourcing tasks and responsibilities incurred by outsourced parties, and to reach a mutual agreement on details of information security measures.

To execute administrative tasks using services such as free internet data processing services provided by the private sectors under general terms and conditions, which is one of the services under “external services on general terms and conditions” defined in section 1.3, is also considered as a form of outsourcing. When using such services, the tasks should be limited to those involve no confidential information handling which require no high level of information management at the outsourcing parties, and “Use of external services on general terms and conditions” in paragraph 4.1.2 can be applied in lieu of provisions in this section.

Scope

<Examples of outsourcing>

- Development and construction of information systems
- Development of application programs and website contents (hereinafter referred to as “applications and contents), and so on.
- Operation of information system
- Information processing using external services such as public cloud services
- Operation support services (statistics, data aggregation, data entry, media conversion, and so on.)
- Project management support services
- Investigation and research (investigation, research, examination, etc.)
- Leasing of information systems, data centers, and telecommunication lines

Compliance Requirements

(1) Maintenance/establishment of provisions related to outsourcing

(a) The head information security officer shall maintain/establish provisions related to outsourcing which include the following items.

(i) Criteria for determining the scope of information systems that can be outsourced, as well as the scope of information and information systems that may be accessed by outsourcing parties.

(ii) Criteria and procedures for selecting outsourcing parties.

(2) Contracts related to outsourcing.

(a) When outsourcing tasks, information system security officers or division/office information security officers shall select outsourcing parties in accordance with the criteria and procedures for selection. Implementation of the below specified information security measurements by outsourcing parties shall be the terms of selection, which should be included in the contractual specifications.

(i) Prohibition of use of information by outsourcing parties for non-job related purposes.

(ii) Implementation and management systems of information security measures carried out by outsourcing parties.

(iii) Management systems to prevent any alternation of data and so on, made against the government agencies' intention, by outsourcing companies and their employees, or subcontractors or any other parties, while executing outsourced tasks.

(iv) Information of outsourcing parties including their capital ties, executives, the sites where outsourced tasks are processed, professional affiliations and expertise (qualifications and training experience on information security), experience and nationality of employees of the outsourcing parties.

(v) Measures (including framework and procedures) for information security incidents

(vi) Systems for checking implementation status of information security measures as well as other matters in the contract.

(vii) Remedial actions in case of insufficient implementation of information security measures.

(b) Information system security officers or division/office information security officers shall examine matters such as the classification of information handled by the outsourcing parties and include the following items in the contractual specifications as necessary.

(i) Agreement to undergo information security audits

(ii) Service level assurance

(c) In case that outsourcing parties will subcontract a part of outsourced tasks, information system security officers or division/office information security officers shall make sure the outsourcing parties implement the above specified measures (a) and (b), to ensure a sufficient level of information security against the threats caused by subcontracting.

(3) Implementation of measures by outsourcing parties

(a) Information system security officers or division/office information security officers shall check implementation status of information security measures implemented by outsourcing parties based on the contract.

(b) Information system security officers or division/office information security officers shall take necessary measures such as stop using outsourcing services, and make outsourcing parties to take necessary measures based on the contract, in case that they become aware, or are informed by employees, of information security incidents or use of information for non-job related purposes by outsourcing parties while executing outsourced tasks.

(c) Information system security officers or division/office information security officers shall ensure the information handled by outsourcing parties to be returned or erased upon the termination of the contract.

(4) Information handling when outsourcing tasks

(a) Employees shall comply with the following requirements when providing information and so on, to outsourcing parties.

(i) When providing classified information to outsourcing parties, restrict it to the minimum and use a prescribed safe delivery method.

(ii) When the provided classified information is no longer required by outsourcing parties, make sure the outsourcing parties will duly return or erase the information.

(iii) Immediately report to information system security officers or division/office information security officers in the event of information security incidents or use of information for non-job related purposes while outsourced operations are being performed.

4.1.2 Use of external services on general terms and conditions

Purpose

When executing administrative tasks through outsourcing, it is necessary in principal to ensure proper implementation of information security measures by taking actions such as signing a special contract which contains items set forth in paragraph 4.1.1 “Outsourcing”, with outsourcing parties. However, in those cases where no confidential information handling is involved and no high level of information security management is required, the use of services such as free of charge information processing services provided by the private sector defined in section 1.3 “external services on general terms and conditions” can be considered. When using these services out of necessity, it is vital to make decisions after careful consideration of the potential risks, and take appropriate information security measures in accordance with the compliance requirements set forth in this section.

Compliance Requirements

(1) Maintenance/establishment of provisions related to use of external services on general terms and conditions

(a) The head information security officer shall establish/maintain provisions related to use of external services which contain the following items, and stipulate that no confidential information should be handled when using such services.

(i) Scope of administrative affairs tasks which allows use of external services on general terms and conditions

(ii) Types of external services used for tasks
(iii) Procedures for use and operational steps

(b) Information security officers shall designate officers in charge of each service when using external services on general terms and conditions.

(2) Implementation of measures for use of external services on general terms and conditions

(a) When applying for the use of external services on general terms and conditions, employees shall make sure that the risks of using such services are tolerable, by checking the terms and conditions and other terms of the services, and ensure that the appropriate measures are implemented upon using those services.

4.1.3 Dissemination of information via social media services

Purpose

A variety of social media services including blogs, social networking services, and video sharing sites are widely used on the internet, through which users disseminate and formulate information. These services are now being used by government agencies for proactive public relations activities and other purposes. However, there is the unavoidable risk of impersonation of government agencies' accounts when using such social media services, because they are only available with external services on general terms and conditions, where the government agencies domain names are inapplicable.

Furthermore, there is the possibility of hijacking of government agencies' accounts, as well as a situation where vital information cannot be disseminated due to unannounced discontinuation of these social media services. Therefore, when widely disseminating important information such as vital information, it is necessary to disseminate information in a way that the citizens can access the original information sources, by taking measures such as publishing the information in government agencies' websites while concurrently using the social media services. In addition, the originator of the information needs to implement measures against threats such as impersonation, to protect parties including the citizen from confusions caused by false information.

These social media services undergo rapid technology developments such as functionality expansion and additional services, so it is essential to promptly respond to changes in these external environments, including the business trends of the providers of such services.

Compliance Requirements

(1) Measures for dissemination of information via social media services

(a) The head information security officer shall establish information security measures related to operational procedures which include the following items, giving the fact that the social media services are used with the accounts managed by government agencies.

(i) Measures to prevent impersonation, such as to clearly indicate the organization which manages the accounts, in order to assure the information disseminated from accounts of government agencies is genuinely originated from authentic government agencies

(ii) Measures to prevent unauthorized access, such as proper management of passwords and other information for user/entity authentication

(a) When using social media services at government agencies for information dissemination, information security officers shall appoint personnel in charge of each social media service.

(b) When using social media services to provide vital information to the citizen, employees shall make such information available for viewing on their own government agencies' websites.

Chapter 5 Lifecycle of Information Systems

5.1 Maintenance of Documents and Inventories of Information Systems

5.1.1 Maintenance of documents and inventories of information systems

Purpose

To sustain the level of information security of information systems managed by government agencies, and to appropriately, as well as promptly respond to information security incidents, it is vital to centrally examine the details of information security measures for said systems in the information system inventories. It is also important to regularly manage the information such as procurement specifications and settings of system components in a written format, and to be aware of where to locate them, in order for said information to be promptly referred to when necessary.

Compliance Requirements

(1) Maintenance of information system inventories
   (a) The head information system security officer shall establish/maintain the matters concerning the security requirements for all the information systems in the information system inventories.
   (b) When newly constructing or updating an information system, information system security officers shall record or state the contents of the security requirements described in the information security inventory of said system, and report them to the head information security officer.

(2) Maintenance of documents related to information systems
   (a) Information security officers shall maintain documents required to implement information securities measures for the information systems under their management, containing all the items specified below.
      (i) Information of the server equipment and terminals composing the information systems
      (ii) Information of the communication lines and communication equipment composing the information systems
      (iii) Procedures to maintain the security level of information security of each component of the information systems
      (iv) Procedures when detecting information security incidents

5.1.2 Establishment/maintenance of provisions related to procurement of equipment, etc.

Purpose

Confidentiality, integrity and availability of information processed by information systems may be compromised if a procured equipment lacks required security functions, or any malicious alternation was made during its manufacturing process, or in those cases where information security measures cannot be continuously implemented to the procured equipment.

To address these issues, it is necessary to establish/maintain criteria for selecting equipment etc., as well as procedures for checks and inspections at the time of delivery, to ensure the procurement is

made in accordance with the standards for measures for government agencies.

Compliance Requirements

(1) Maintenance of provisions related to procurement of equipment, etc.

(a) The head information security officer shall establish/maintain the criteria for selecting equipment, etc. The criteria should contain, if necessary, a scheme which enables government agencies to monitor the management of equipment to ensure no malicious alternation is made throughout the lifecycle of equipment, such as its development phase.

(b) The head information security officer shall maintain the checks and inspections procedures at delivery of equipment, etc., considering perspectives of information security measures.

5.2 Measures at Each Phase of Information System Lifecycle

5.2.1 Planning, and definition of requirements for information systems

Purpose

To appropriately maintain information security throughout the lifecycle of information system, it is necessary, at the planning stage of the information system, to establish frameworks which enable information security maintenance, as well as to define requirements for various information security risks at each phase of lifecycle of information system.

Ambiguous, excessive, or insufficient security requirements may result in disadvantages such as cost increase due to excessive measures for information security, unfair competitive biddings caused by different proposal contents due to widely varied interpretations of requirements, and rework in designing and development, as well as information security incidents after commencement of operations.

Therefore, it is important to review measures for expected threats against information systems and to appropriately include sufficient security requirements in specifications, after taking consideration of the scope of tasks, information handled, users who handle the information, as well as the environments and methods and so on used for information processing.

In addition, it is vital to examine the measures to protect the information systems to be constructed from vulnerabilities at the planning phase of the systems, before its construction.

The provisions in section 4.1.1 “Outsourcing” shall also be observed when outsourcing construction, operation, and maintenance of information systems.

Compliance Requirements

(1) Ensuring the implementation of frameworks

(a) Information system security officers shall request persons responsible for managing information systems to ensure the implementation frameworks which enable to maintain the information security throughout the information system's lifecycle.

(b) When constructing a system based on the common platform which serves as a foundation for constructing an information system, information system security officers shall maintain said system, and request persons responsible for the management of information systems

to establish frameworks in accordance with the operational management provisions and so on, set forth by the government agencies which maintain, operate and manage the common platform which serves as a foundation for constructing an information system.

(2) Formulation of security requirements for information systems

(a) Information system security officers shall formulate security requirements including the following items, based on the matters such as purpose of constructing the information system, task requirements for the targeted tasks and so on, as well as classification of information handled by said system.

(i) Requirements for security functions to be incorporated to the system such as user/entity authentication, access control, authority control, log management, and encryptions

(ii) Requirements for operational management functions such as monitoring, while the information systems are in operation.

(iii) Requirements for measures against vulnerabilities of the information systems

(b) Information system security officers shall formulate security requirements based on the "Guidelines on Risk Assessment and Digital Signature/Authentication for e-Government" for the systems which offer online procedures such as applications and reports transmitted between citizens/corporations and the government.

(c) Information system security officers shall refer to the "List of Requirements for Ensuring Security in Procurement of IT Products" when procuring an equipment, and shall analyze the threats in the environments where the equipment is used, and formulate security requirements to counter the information security threats in said equipment, etc.

(d) When constructing systems based on the common platform which serves as a foundation for constructing an information system, information system security officers shall formulate security requirements in accordance with the operational management provisions and so on related to the security measures for such common platform, in order to maintain the level of information security of entire common platform system.

(3) Measures when outsourcing construction of information systems

(a) When outsourcing construction of information systems, information system security officers shall oblige the outsourcing parties to ensure compliance on the following requirements by implementing measures such as indicating them in the procurement specifications

(i) Appropriate implementation of information security requirements

(ii) Systems tests conducted from perspectives of information security

(iii) Information security measures in the environment and process of information system development.

(4) Measures when outsourcing operation and maintenance of information systems

(a) When outsourcing operation and maintenance of information systems, information system security officers shall ensure the outsourcing parties to comply with the requirements for proper operation of the system's security functions, by indicating these requirements in the procurement specifications, and so on.

5.2.2 Procurement and construction of information systems

Purpose

When procuring and constructing information systems, it is necessary to procure an equipment based on the selection criteria and to carry out information system measures at the development phase of the system, in order to appropriately implement information security measures in accordance with the prescribed security requirements.

It is also required to conduct system inspections following the established/maintained inspection procedures at the time of delivery or reception of information systems, to ensure appropriate incorporation of security and management functions to protect the information handled by such systems.

Compliance Requirements

(1) Measures when selecting equipment, etc.
   (a) Information system security officers shall validate if the equipment, etc.is conformed to its selection criteria and use the result as one of the factors for its selection.

(2) Measures when constructing information systems
   (a) When constructing information systems, information system security officers shall implement measures deemed necessary from perspectives of information security.
   (b) When the constructed information systems are migrated to the operation and maintenance phase, information security officers shall implement the measures for procedures and environments of migration deemed necessary from perspectives of information security.

(3) Measures for inspections on delivery
   (a) Information system security officers shall conduct validations and inspection at the time of delivery, following the inspection procedures prescribed in the specifications and so on, in order to ensure the procured equipment, etc. and the received information systems are conforming to the requirements for information security measures.

5.2.3 Operation and maintenance of information security

Purpose

When information systems are migrated to the operational phase, it is necessary to establish the resource allocation system in operation, and to perform regular checks of parameters settings on the equipment and other components, as well as to manage records of operation and maintenance, in order to ensure proper implementation of the security requirements determined upon planning, procurement, and construction of the system.

Most of information security incidents normally occur during operation, so it is important to duly monitor the operation of information systems to confirm effectiveness of the implemented information security measures.

Also, the information security measures for system maintenance need to be appropriately

implemented in the same manner as those for system operation. In those cases such as individually outsourcing system maintenance work, it is essential to duly implement the information security measures in accordance with the standards for measures for government agencies.

Compliance Requirements

(1) Measures for information systems during operation and maintenance
   (a) Information system security officers shall appropriately operate the security functions incorporated to the system during its operation and maintenance.
   (b) For the systems constructed based on the common platform which serves as a foundation for constructing an information system, information system security officers shall appropriately operate the information systems under the operational management framework in accordance with the segregation of duties with the other government agencies which maintain, operate and manage the common platform system. Information system security officers shall also operate the information systems following the common platform system's operational management provisions and so on, in order to maintain the level of information security of entire common platform system.
   (c) Information system security officers shall manage the records of operation and maintenance, in order to facilitate tracing of incidents such as malicious activities and unintended access to the systems.

5.2.4 Update and disposal of information systems

Purpose

When updating or disposing of information systems, it is necessary to prevent leakage of highly confidential information contained in the system during disposal or recycling.

If the highly confidential information is saved on the information systems, or classifications or handling restrictions of information stored on the systems are unclear, it is essential to implement measures to ensure complete erasure of such information.

Compliance Requirements

(1) Measures for update and disposal of information systems
   (a) When updating or disposing of information security systems, information security officers shall implement the following measures, taking into account of classifications and handling restrictions of the information stored in said systems.
      (i) Information security measures for transferring data when updating information security systems.
      (ii) Erasure of unnecessary data when disposing of information security systems

5.2.5 Review on measures for information systems

Purpose

As the environments surrounding information security are constantly changing, the level of information security cannot be maintain if emerging threats are not precisely addressed. For this reason, it is necessary to regularly review the information security measures, and conduct further reviews in the event of drastic changes in external environments, and so on.

Compliance Requirements

(1) Review on measures for information systems
   (a) Information security officers shall duly examine necessity of review on information security measures on information systems, in response to the status such as emerging threats, operation, and monitoring, and take necessary measures if they are deemed necessary.

5.3 Operational Continuity Plan of Information Systems

5.3.1 Ensuring consistency between information security measures for information systems and the systems' operational continuity plans

Purpose

It is essential, even in emergency, to ensure continuity of business whose interruption may cause a serious threat to the safety and benefit of citizens, so that government agencies duly establish and carry out business continuity plans.

On the other hand, when continuing operation of information systems at the time of emergency, it is vital to examine and determine the measures for information security in emergency.

It is also necessary to ensure that the requirements prescribed in the business continuity plan and information system operational continuity plan, and those prescribed in the information security related provisions are in accordance with each other, and contain no inconsistencies.

Compliance Requirements

(1) Ensuring consistency between information security measures for information systems and the systems' operational continuity plans
   (a) Upon maintaining the information system operational continuity plan for the system which supports the highly prioritized tasks in emergency at government agencies, the head information security officer shall review the measures for information systems in emergency.
   (b) The head information security officer shall confirm if the measures for information systems in emergencies are feasible, when performing tasks such as education and training as well as maintenance and revision on the operational continuity plan of information systems.

Chapter 6 Security Requirements for Information Systems

6.1 Security Functions of Information Systems

6.1.1 User/entity authentication functions

Purpose

To prevent information security incidents, such as leakage or loss of information, suspension of information systems and so on caused by unauthorized access, the information systems should be equipped with the user/entity authentication functions.

Users of information systems at government agencies are not limited to employees, such as users of services for general public. Therefore, it is necessary to protect identification codes and user/entity authentication information regardless of user types, while implementing measures to make users aware of precautions to take.

Compliance Requirements

(1) Implementation of the user/entity authentication functions

(a) Information system security officers shall implement the user/entity identification and authentication functions when identification and verification of authorized users/entities are necessary to control the access to information systems and information.

(b) Information system security officers shall implement measures to prevent malicious activities caused by leakage of user/entity authentication information and so on, as well as the measures against unauthorized attempts of user/entity authentication.

6.1.2 Access control functions

Purpose

In case that multiple users operate information systems, access to some specific information should be limited only to relevant users who require such information for their job functions. Therefore, it is essential to ensure appropriate access control on the information systems, restricting which user is allowed to access which information.

Compliance Requirements

(1) Implementation of access control functions

(a) Information system security officers shall implement a user-dependent access control function when it is necessary to restrict access to certain information handled by the system.

(b) When introducing access control functions, information system security officers shall establish information security related requirements for access control, including restrictions based on profiles of users and user groups, as well as restrictions by usage hours and terminals and so on, taking into account the resiliency and usability of the information security.

(2) Enforcement of appropriate access control
   (a) Information system security officers shall appropriately perform access control in accordance with the classification and handling restrictions of the information to be stored on the information systems whose access control cannot be performed by employees themselves.

6.1.3 Authority control functions

Purpose

Administrator authority is one of the authority control functions on the information system, which generally includes privileges to allow all operations on the system.

If such privileges were stolen by malicious third parties, there would be dangers such as leakage or manipulation of user/entity authentication information, or disabling of information security functions by unauthorized setting changes on the information system.

Therefore, in order to limit the administrator authority only to the relevant users and to prevent its misuse, it is vital to implement authority control functions to the system.

Compliance Requirements

(1) Implementation of authority control functions
   (a) Information system security officers shall implement authority control functions which enable management of authority control on the information system, when it is necessary to verify the authenticity of a user/entity of said system.
   (b) When implementing authority control functions, information system security officers shall implement measures to minimize damages caused by thefts of administrator's privileges, and to prevent malicious and erroneous operations which are internally performed.

(2) Granting and managing identification codes and user/entity authentication information
   (a) Information system security officers shall implement appropriate measures to grant identification codes and user/entity authentication information to the users/entities of information systems, as well as the measures to have such information to be duly managed.

6.1.4 System logs retrieval and management

Purpose

Logs of the information system are the records of operation, user access history, and other essential information of the system, which are important tools for detecting information security incidents including signs of an incident, such as unauthorized access and operations by malicious third parties. If any incident concerning information security on the system takes place, these logs will serve as important material for identifying and clarifying the causes in the course of investigations after the incident. For this reason, information systems' logs should be duly retrieved in accordance with system specifications and need to be appropriately maintained and protected to prevent these logs from being manipulated or lost.

Compliance Requirements

(1) Event logs retrieval and management

(a) Information system security officers shall retrieve logs of information system when he or she needs to verify the information systems are appropriately used and free from unauthorized access and operation.

(b) Information system security officers shall determine items such as types of information recorded in the log, storage periods, log information handling methods from a viewpoint of classified information handling, as well as measures to implement when log retrieval is not possible, and appropriately manage the logs.

(c) Information system security officers shall establish a function to examine or analyze the logs retrieved from the information systems, and perform examinations or analysis to detect unauthorized access and operations, etc. by malicious third parties, and so on.

6.1.5 Encryption and digital signatures

Purpose

Encryption and digital signatures are effective means to prevent leakage and manipulation of information handled by information system, so it is essential to appropriately implement these functions to the system.

When introducing encryption and digital signatures, it is necessary to take into account the issues such as adequacy of algorithms, measures in case that said algorithm was compromised during operation, as well as appropriate key information management.

Compliance Requirements

(1) Implementation of encryption and digital signature functions

(a) Information system security officers shall take the following measures to prevent leakage and manipulation of information handled by information systems

(i) Examine the necessity of encryption functions for the information systems handling confidential information, and duly implement them when it is deemed necessary.

(ii) Examine the necessity of digital signature and verification functions for the information systems handling critical information, and implement them when it is deemed necessary.

(b) Information system security officers shall refer to the “e-Government Recommended Ciphers List” whose security and performance is confirmed by CRYPTREC (the Cryptography Research and Evaluation Committees) and shall establish operational methods of encryption and digital signature algorithm used on information systems, which include the following items.

(i) For encryption and digital signature algorism used by employees, ensure the one in the “e-Government Recommended Ciphers List” (CRYPTREC) is to be applied where possible.

(ii) When introducing encryption or digital signature upon implementations or updates of information systems, apply algorithms in the “e-Government Recommended Ciphers List”, expect for unavoidable circumstances.

(iii) Establish emergency response procedures in the event that the algorithm is compromised.

(iv) Establish procedures for managing keys for decryption of encrypted information, and for granting digital signatures

(c) When assigning a digital signature, information security officers shall ensure use of the digital certificate issued by the Government Public Key Infrastructure, if the one which is applicable and serves the purpose of digital signature is available with the GPKI, after examining the algorithm and operational methods of encryption and digital signature applied at their own government agencies.

(2) Management of encryption and digital signature

(a) Information system security officers shall take the following measures to ensure proper use of encryption and digital signature

(i) For the information systems which assign digital signatures, securely provide the verifiers of signatures with information and methods of verifying the validity of the signatures

(ii) For the information systems which perform encryption, or those which perform assignment or verification of digital signatures, regularly obtain information on threats which compromise the algorithm selected for such operations, and share it with employees as necessary.

6.2 Measures against Information Security Threats

6.2.1 Measures against software vulnerabilities

Purpose

Potential threats against information systems of government agencies include attacks such as third party intrusions to the systems causing theft or destructions of important government information, as well as suspension thereof due to excessive workloads imposed by the third party. In particular, third party intrusions made to services for the general public resulting in personal information leakage would undermine public trust in the government.

As for these types of threats in general, attackers are likely to abuse vulnerability of software in the server, terminals, and communication line equipment which compose of information systems. Therefore, for information systems in government agencies, it is necessary to quickly and appropriately take measures against software vulnerabilities.

By the same token, the hardware of information systems may contain such vulnerabilities, so it is essential to refer to the provisions in section 5.2.2 “Information system procurement and configuration”, and to implement necessary measures.

Compliance Requirements

(1) Implementation of measures against software vulnerabilities

(a) When installing or starting operations of servers, terminals, and communication line equipment, information system security officers shall implement measures against publicly disclosed vulnerabilities of the software used on said equipment.

(b) When the publicly disclosed information about vulnerabilities is yet to be known, and applicable measures for servers, terminals, and communication line equipment are available, information system security officers shall implement such measures.

(c) When the information about vulnerabilities of the software used on servers, terminals, and communication line equipment becomes available, information system security officers shall apply security patches, or establish plans for addressing software vulnerabilities and implement measures, after examining the effects upon software updates and so on.

(d) Information system security officers shall regularly verify the implementation status of measures against vulnerabilities of software, including the tailor made software used on servers, terminals, communication line equipment, and establish countermeasures if any vulnerabilities with no relevant measures are identified.

6.2.2 Measures for protection against malware

Purpose

If information systems were infected by malware, potential threats would be system breakdown and leakage of important information stored on said systems. Moreover, such infected information systems can spread infections to other systems, and possibly used as a platform to send spam e-mails and for denial-of-service attacks and so on, as well as a source of targeted attacks, which could give a threat to other entities and other information systems.

In order to prevent such incidents from occurring, it is necessary to duly implement measures against malware.

Compliance Requirements

(1) Implementations of measures against malware

(a) Information system security officers shall install anti-malware software and other tools on server equipment and terminals. However, this shall not apply when no anti-malware software and so on, which are operational on said server equipment and terminals is readily available.

(b) Information system security officers shall take measures against malware, such as installing anti-malware software to protect all possible malware infection routes.

(c) Information system security officers shall regularly examine the implementation status of measures against malware as needed and take necessary measures.

6.2.3 Measures against denial-of-service attacks

Purpose

Potential threats against information systems accessed through the internet would be a denial-of-service attack by third parties, which disables legitimate users to access the services. Therefore, for information systems of government agencies which are accessed through the internet, it is vital to take denial-of-service attacks into account and duly implement measures to ensure continuous availability of the systems.

Compliance Requirements

(1) Implementation of measures for denial-of-service attacks

(a) For information systems (referring to only those systems accessed through the internet, hereinafter the same in this section) handling vital information, system security officers shall implement measures for denial-of-service attacks, by using the functions incorporated in the equipment necessary for providing such services, like server equipment, terminals, and communication line equipment, or the methods offered by private business providers, and so on.

(b) For information systems handling vital information, system security officers shall construct information systems equipped with tools which minimize impacts of denial-of-service attacks.

(c) For information systems handling vital information, system security officers shall identify equipment to be monitored among the server equipment, terminals, communication line equipment, and communication lines which are subject to denial-of-service attacks, and conduct monitoring.

6.2.4 Measures against targeted attacks

Purpose

Targeted attacks are attacks targeting a specific organization, where attackers conduct a thorough investigation in advance, on the matters such as business practices and other internal information of the target, then make tenacious attacks with a combination of various types of attacks, applying the most effective method to violate the target organization.

A typical and likely example of such attacks is the one made by intruding into a system of certain organization, then expand the intrusion areas to stole or destroy their critical information. A series of such attacks are also made by using unknown methods, which make it difficult to perfectly detect and prevent them.

Therefore, it is necessary to be prepared for targeted attacks by establishing the multiple protection system for information security, which consists of measures to reduce targeted attack intrusions against the organization (gateway measures), and measures for early detection and response to the intrusions, and measures to make expansion of intrusions harder, as well as measures for detection and response to unauthorized communications with external entities (inter-organizational measures).

Compliance Requirements

(1) Implementation of measures for targeted attacks
   (a) Information security officers shall implement measures for information systems which reduce targeted attacks intrusions against the organization (gateway measures).
   (b) Information security officers shall implement measures for information systems to immediately detect and respond to the intruded attacks, and to make expansion of the intrusion harder, as well as to detect and respond to unauthorized communication with external entities (internal measures).

6.3 Creation and provision of applications and contents

6.3.1 Measures upon creating applications and contents

Purpose

Government agencies prepare applications and contents and make them widely available to offer administrative services such as providing information, executing administrative procedural tasks, and collecting opinions. The information security level of user's terminal should not be deteriorated when using these applications and contents. Government agencies need to implement information security measures when providing applications and contents. In addition, when outsourcing development and provisions of applications and contents, the requirements in section 4.1.1 "Outsourcing" should be observed.

Compliance Requirements

(1) Establishment/maintenance of provisions related to creation of applications and contents
   (a) The head information security officer should maintain provisions to prevent actions which cause deterioration of information security level of the systems other than those of their own government agencies when providing applications and contents.
(2) Formulation of security requirements for applications and contents
   (a) Information security officer shall include the following items in the specifications of applications and contents, in order not to deteriorate the level of information security of the users other than those of their own government agencies.
      (i) Applications and contents to be provided shall contain no malware.
      (ii) Applications and contents to be provided shall contain no vulnerability.
      (iii) The contents shall not be provided in the executable program format, unless there is no other way to provide them.
      (iv) If there is any mean to verify that the applications and contents are authentic and free from manipulation, such as digital certificate and likewise is available, it shall be provided to the recipients of the applications and contents.
      (v) When developing applications and contents, methods of providing them shall be selected to ensure the users of the OS and software will not be prompted to change the setting which might deteriorate the information security level, including the changes which force them to use the OS version and software, etc. with vulnerabilities.

(vi) Applications and contents should be developed ensuring not to contain such functions which allow the third parties to obtain the information of service users and other parties against their will, which are not essential for utilizing the service.

(b) When outsourcing applications and contents development and creation, employees shall include the requirements in the preceding items in the procurement specification.

6.3.2 Measures upon providing applications and contents

Purpose

Government agencies prepare websites and make them available to citizens to offer administrative services such as providing information, executing administrative procedural tasks, and collecting opinions. As these services are normally provided through the internet, it is important for citizens to be sure that these services are genuinely offered by authentic government agencies. Furthermore, if no measures are taken against websites which impersonate government agencies, there would be a fear that the public trust for them would be undermined, and also that the citizens could be directed to unauthorized websites, and infected with malware. Therefore, it is essential to implement measures to respond to such situations.

Compliance Requirements

(1) Use of government domain name

(a) Information system security officers shall specify the use of .go.jp domain name (hereinafter referred to as “government domain name”) in the information systems specifications, so that the users other than those of own government agencies can confirm that the websites are provided by a genuine government agency. However, this shall not apply to what is set forth in section 4.1.3.

(b) When outsourcing the creation of a website targeting the users other than those of own government agency, the use of government domain name shall be specified in the procurement specifications, as stated in the preceding items.

(2) Prevention of users from being lured to malicious websites

(a) Information system security officers shall implement measures to prevent users from being lured, through pages such as search engine sites, to malicious websites which impersonate government agencies.

(3) Notification of applications and contents provided by the parties other than their own government agencies

(a) When notifying users of applications and contents provided by the parties other than their own government agencies, employees shall implement the following measures.

(i) Clearly specify the name of organization which manages the applications and contents

(ii) Clearly specify when the location of applications and contents was validated (including the expiry date of the URL domain name to which the sites are linked, and so on), or the guaranteed validation period.

(iii) When sending such notifications by e-mail, an e-mail address with a government domain name shall be clearly specified as a contact for inquiries about notification, or a digital signature with a government domain name shall be included in the notification e-mail.

Chapter 7 Information Systems Components

7.1 Terminals, Server Equipment

7.1.1 Terminals

Purpose

When using terminals, there are risks such as leakage of stored information due to external causes, such as malware infection and intrusions. Moreover, internal causes such as improper system handling or negligence of employees might result in information security incidents, including malware infection. As for mobile terminals, there is a higher risk of information leakage caused by theft or loss and so on, of the device. These issues should be taken into consideration when implementing measures.

In addition to the compliance requirements in this section, requirements regarding measures for functions such as user/entity authentication, access control, authority control, and log management in section 6.1 “Security Functions for Information Systems”, section 6.2.1 “Measures against software vulnerabilities”, section 6.2.2 “Measures for protection against malware”, and section 7.3.2 “IPv6 communication lines” should also be complied with.

Compliance Requirements

(1) Measures when introducing terminals

(a) For terminals which handle classified information, information system security officers shall implement measures against physical threats such as theft and unauthorized removal of terminals, unauthorized use of terminals by malicious third parties, as well as unauthorized viewing of display devices of terminals.

(b) For mobile terminals handling confidential information outside of the areas requiring control measures, information system security officers shall implement measures to prevent information from being stolen by malicious third parties in case of theft of terminals, and so on.

(c) To eliminate the possible increase in vulnerability due to use of variety of software, information system security officers shall specify the software which is approved, or prohibited to be used on the terminals.

(2) Measures when operating the terminals

(a) Information system security officers shall periodically conduct a review of software which is approved, or prohibited to be used on the terminals.

(b) Information system security officers shall periodically verify the status of all software used on the terminals under their management, and implement corrective measures when identifying any terminal in inappropriate status, and so on.

(3) Measures when terminating the operation of terminals

(a) Information system security officers shall erase all the information stored on the external storage media of the terminal when terminating its operation.

7.1.2 Server equipment

Purpose

Server equipment such as e-mail servers, webservers, and file servers normally store large size of information, so that the impact of leakage and manipulation of such information is far larger than that of terminals. In addition, server equipment are subject to a higher risks of malware infection and intrusions, because their functions are generally utilized via communication lines. If the server equipment at government agencies were used for unauthorized access or relaying spam e-mails, it would seriously undermine the public trust in government agencies.

Moreover, as a large number of users simultaneously use server equipment, failure of its functions would result in a greater impact. These issues should be taken into consideration when implementing measures.

In addition to the compliance requirements in this section, requirements regarding measures for functions such as user/entity authentication, access control, authority control, and log management set forth in section 6.1 “Security Functions for Information Systems”, as well as compliance requirements concerning server equipment set forth in section 6.2.1 “Measures against software vulnerabilities”, section 6.2.2 “Measures for protection against malware”, section 6.2.3 “Measures against denial-of-service attacks”, and section 7.3.2 “IPv6 communication lines” should be complied with. For e-mail servers, webservers, and DNS servers in particular, the compliance requirements set forth in section 7.2 “E-mails, Web, and so on” should be complied with, in addition to the common measures stipulated in this section.

Compliance Requirements

(1) Measures when implementing server equipment

(a) For server equipment which handles classified information, information system security officers shall implement measures against physical threats such as theft and unauthorized removal of server equipment, unauthorized use of server equipment by malicious third parties, as well as unauthorized viewing of display devices of server equipment.

(b) To prevent situations where services are suspended due to failure, excessive access, and other problems with information systems which handle vital information, information system security officers shall, considering the future prospects, ensure system’s availability by setting up the server equipment for such services in a redundant configuration, and so on.

(c) To eliminate the possible increase in vulnerability due to use of variety of software, information system security officers shall specify the software which is approved, or prohibited to be used on the server equipment.

(d) Information system security officers shall implement measures to prevent leakage of information sent and received while the server equipment maintenance is being performed via communication lines.

(2) Measures when operating the server equipment

(a) Information system security officers shall periodically conduct a review of software which is approved, or prohibited to be used on the server equipment.

(b) Information system security officers shall periodically verify the software and configuration of all server equipment under their management, and implement corrective measures when identifying any server equipment in inappropriate status, and so on.

(c) Information system security officers shall implement measures to monitor the occurrence of unintended incidents such as malicious acts and unauthorized access to the server equipment. However, this shall not be applied if such monitoring is deemed unnecessary due to the usage environment of the server equipment.

(d) For server equipment handling vital information, information system security officers shall implement measures which enable to recover the server equipment, such as to get the information back-up.

(3) Measures when terminating the operation of server equipment

(a) Information system security officers shall delete all information stored on the external storage media of server equipment when terminating its operation.

7.1.3 Multifunction devices and equipment for specific purposes

Purpose

Multifunction devices containing a combination of printer, fax, image scanner, and copier functions (hereinafter referred to as “multifunction devices”) are used at government agencies. These multifunction devices are often connected to internal communication lines, as well as to the public telephone networks and other communication lines when in use, in which case a various kinds of threats are expected, because many services including web console, file transfer, file sharing, as well as remote maintenance will be operating on such devices.

Moreover, information systems for specific purposes, such as systems for video conference, IP phone, and network camera, are also used at government agencies. With such information systems, in addition to devices for general purposes, equipment for specific purposes dedicated to the system are sometimes used, in which case there are possible threats depending on factors such as the characteristics, information handled, methods of use, as well as connection types of communication lines, of such equipment.

Therefore, it is important to treat these multifunction devices and equipment for specific purposes as part of the information system components, and to implement appropriate measures by assigning personnel and clarifying who is in charge.

Compliance Requirements

(1) Multifunction devices
   (a) When procuring multifunction devices, information system security officers shall establish appropriate security requirements according to functions, installation environments, as well as classification and handling restrictions of information handled by such devices.
   (b) Information system security officers shall implement measures for information security incidents against multifunction devices while in operation, by taking actions such as to appropriately set up the functions available on said devices.
   (c) Information system security officers shall delete all information stored on the external storage media of multifunction device when terminating its operation.

(2) Equipment for specific purposes
   (a) For equipment for specific purposes, if there are possible threats depending on information handled, methods of use, and connection types of the communication lines and so on, information system security officers shall implement measures suitable for the characteristics of said equipment

7.2 E-mail, Web, and others

7.2.1 E-mail

Purpose

As sending and receiving e-mails is nothing but an exchange of information, there are risks against confidentiality, including information leakage caused by inappropriate use, as well as risks that employees who use e-mail to be victimized by illegal acts abusing e-mails, such as impersonation by malicious third parties. In order to prevent these problems, proper e-mail server management is essential.

In addition to the compliance requirements in this section, the same for the server equipment in section 7.1.2 “Server equipment” should be complied with.

Compliance Requirements

(1) Measures when introducing e-mail services
   (a) Information system security officers shall set up the e-mail servers, ensuring no illegal e-mail relaying occurs.
   (b) Information system security officers shall provide functions of user/entity authentication when sending and receiving e-mails between e-mail clients and servers.
   (c) Information system security officers shall implement measures to prevent e-mail spoofing.

7.2.2 Web

Purpose

Webservers are open to public access on the internet and under constant risk of attacks. Possible

damage include manipulation of web contents (information published on web pages), and webservers to be made unavailable or intruded, so it is necessary to address such damage by combining appropriate measures and implement them.
In addition to compliance requirements in this section, the same for the server equipment in section 7.1.2 “Server equipment” should be complied with.

Compliance Requirements

(1) Measures when introducing and operating webservers
   (a) For management and setting of webservers, information system security officers shall implement measures to ensure information security, including the following items.
      (i) Unnecessary functions of webservers shall be stopped or restricted
      (ii) Personnel responsible for editing web contents shall be limited.
      (iii) Manage web contents to ensure no senseless nor prohibited contents shall be published.
      (iv) Terminals used for editing web contents shall be restricted, and ID codes and user/entity authentication information shall be appropriately managed.
      (v) If it is necessary to prevent information leakage caused by tapping and other incidents during communication, such as when communicating service users’ personal data, the functions for encryption and authentication by digital certificates shall be provided.
   (b) Information system security officers shall verify the information saved on webservers, and ensure no information unnecessary for providing services is stored therein.

(2) Measures when developing and operating web applications
   (a) When developing web applications, information system security officers shall implement measures to eliminate known vulnerabilities of existing web applications. In addition, these measures shall be periodically reviewed during operation for any oversights, and appropriate action should be taken when identifying such oversights.

7.2.3 Domain Name Systems

Purpose

A domain name system (DNS: Domain Name System) serves as a base for a network system, which receives queries from clients (DNS clients) including terminals, and returns responses such as corresponding relationships between IP addresses and domain names and host names. If a DNS becomes unavailable, the websites and e-mails which use the host names and the domain names, etc. will be unusable. In addition, if the integrity of information supplied by a DNS is compromised and incorrect information is provided, there is a risk of damage such as DNS clients, including terminals, will be connected to malicious servers. Furthermore, if there is any error in the setting of a DNS, detection of e-mail spoofing becomes impossible, because the DNS partially handles the measure against spoofing of e-mails whose addresses contain the domains managed by the DNS. To avoid such problems, appropriate DNS server management is essential.

In addition to the compliance requirements in this section, the same for server equipment in section 7.1.2 “Server equipment” should be complied with.

Compliance Requirements

(1) Measures when introducing the DNS

(a) For the DNS content servers which provide name resolution to information systems handling vital information, information system security officers shall implement measures to ensure there is no interruption to the name resolution.

(b) For the DNS cache servers, information system security officers shall implement measures to ensure appropriate responses to the name resolution queries.

(c) When the DNS content servers are used to provide the resolution of the names exclusive to their own government agency, information system security officers shall implement measures to ensure no such information is leaked outside of the government agencies.

(2) Measures when operating the DNS

(a) When installing multiple DNS content servers, information system security officers shall maintain consistency among the servers with regards to the information of the domains under their management.

(b) Information system security officers shall periodically verify the accuracy of the information about the domains managed on the DNS content servers.

7.3 Communication Lines

7.3.1 Communication lines

Purpose

Most of unauthorized access and denial-of-service attacks against server equipment and client terminals are carried out through the communication lines and the communication line equipment Therefore, when implementing information security measures for communication lines and communications line equipment, it is necessary to examine potential risks thoroughly and implement measures at the constructing phase of information systems. Types of information security risks vary depending on the communication line providers and the physical line types. These differences should be fully taken into account when implementing measures.

In addition, configuration of the communication lines and conditions of information systems connected to them at the launch of information systems may change after operating them for a certain period of time. Also, there may be some changes in types of attacks.

The measures estimated to be sufficient at the construction phase of information systems may become insufficient, so it is vital to continually implement measures throughout the operation of communication lines.

Compliance Requirements

(1) Measures when installing communication lines

(a) During the communication lines installation, information system security officers shall

select appropriate line types according to the classification and handling restrictions of the information handled by the information systems connected to the communication lines, and implement measures necessary for said lines to prevent impacts of information security incidents.

(b) Information system security officers shall have the communication lines equipped with the functions to perform access control and route control on the server equipment and terminals.

(c) Information system security officers shall implement measures to ensure the confidentiality of communication contents, if assuring the confidentiality thereof is deemed necessary when connecting information systems handling confidential information to the communication lines.

(d) Information system security officers shall implement measures which enable them to confirm that the information system is the one approved to be connected to the communication lines.

(e) Information system security officers shall install communications line equipment in the areas requiring control measures. However, when it is difficult to install them in said areas, measures such as physical protections to keep the equipment from destruction and unauthorized operation by malicious third parties shall be implemented.

(f) Information system security officers shall implement measures to ensure continuous operation of communication lines connected to the information systems handling vital information.

(g) When connecting the internal communication lines to the external communication lines such as internet access lines and public communication lines, information system security officers shall implement measures to ensure the information security of the internal communication lines and the information systems connected to them.

(h) Information system security officers shall implement measures to monitor communication contents sent and received between the internal communication lines and the external communication lines.

(i) Information system security officers shall specify the software required for operating communication line equipment and maintain/establish authorization procedures for changing software. This shall not be applied to the communication line equipment whose software is difficult to change.

(j) Information system security officers shall ensure information security of remote access, where communication line equipment are remotely accessed for maintenance and diagnosis.

(k) When using communication line services of telecommunication carriers, information system security officers shall establish agreements, upon signing a contract with the outsourcing parties who construct information systems, on measures to ensure the level of information security of said line services as well as its service level.

(2) Measures when operating communication lines

(a) Information system security officers shall implement measures required to prevent

information security incidents during the operation of communications line equipment.

(b) Information system security officers shall appropriately perform route control and access control, and review its settings when any change made to the communication lines and the requirements for establishing communication. This review shall also be conducted periodically.

(c) Information system security officers shall periodically check the status of software required for operating communications line equipment, and implement corrective measures if any improper status is detected, such as unauthorized software is installed on the equipment.

(d) In the event of incidents which endanger information security of certain information system, information security officers shall protect other information systems which share the communication lines with the endangered information system, by changing the line configuration to establish a closed and independent communication line, separated from the shared ones.

(3) Measures when terminating the operation of communication lines

(a) When terminating the operation of communication line equipment, information security officer shall take appropriate measures, such as erasing all the information recorded on the external storage media on said equipment to prevent leakage of information stored during the operation, in case that such equipment composing the communication lines are reused or discarded after terminating its operation.

(4) Measures when introducing remote access environments

(a) When installing the VPN lines, information system security officers shall implement measures required to ensure information security, such as user/entity authentication and encryption of communication contents.

(b) When constructing the remote access environments via public telephone networks, information system security officers shall implement measures required to ensure information security, such as user/entity authentication and encryption of communication contents.

(5) Measures when introducing wireless LAN environments

(a) When constructing the internal communication lines with wireless LAN technologies, information system security officers shall, on top of implementing the common measures for communication line construction, encrypt the communication routes to ensure the confidentiality of communication contents, then implement other measures required to ensure information security.

7.3.2 IPv6 communication lines

Purpose

Government agencies have been taking initiatives to comply with the IPv6 communication protocol, but there are many issues to be considered when applying the protocol, such as direct IP reachability and co-existing of two different protocols during the migration from the IPv4 communications protocol.

In recent years, a large number of server equipment, terminal, and communication line equipment, etc. which are equipped with IPv6 communication technology (hereinafter referred to as “IPv6 communications”) by default have been released. When using these products, unintended IPv6 communications could occur on the communication network, which may be abused for unauthorized access. Therefore, necessary measures should be implemented.

There will be further changes in IPv6 technology trends, while the associated information security measures are expected to develop further, making it essential for government agencies to closely watch these technological trends of information security and duly respond to them.

Compliance Requirements

(1) Measures related to information systems with IPv6 communications

(a) When constructing information systems using IPv6 technologies for communication, information system security officers shall select, when possible, a Phase-2 compliant product based on the IPv6 Ready Logo Program, as the equipment, etc. to procure.

(b) For information systems to be constructed are expected to perform communication with IPv6 technology, information system security officers shall take into account the characteristics of IPv6 communication and so on, and review the threats and vulnerabilities including the following items, and shall implement necessary measures.

(i) Threats related to direct IP reachability via global IP addresses

(ii) Threats related to unauthorized access due to incomplete settings of IPv6 communication environments, and so on.

(iii) Vulnerabilities due to lack of consideration for the required process when IPv4 and IPv6 communications coexist in the information system.

(iv) Vulnerabilities due to lack of consideration for the required IPv6 addresses handling on the applications.

(2) Control and monitor for unintended IPv6 communications

(a) When connecting server equipment, terminals and communications line equipment to communication lines for which no IPv6 communication is intended, the information system security officers shall implement measures to control IPv6 communications in order to prevent information security threats caused by unauthorized IPv6 communications received from said lines, such as arrival of unexpected IPv6 communication packets as a result of automatic tunneling functions.

Chapter 8 Use of Information Systems

8.1 Use of Information Systems

8.1.1 Use of information systems

Purpose

Employees use a wide range of information systems, including e-mail, web, and the systems for processing tasks on terminals, in order to execute their duties. There is a risk for information security incidents if these systems are not used appropriately.

Therefore, it is essential to maintain/establish provisions related to the use of information systems, and employees should comply with the provisions when using the systems.

Compliance Requirements

(1) Establishment/maintenance of provisions related to the use of information systems

(a) The head information security officer shall establish/maintain provisions related to information security when using information systems at government agencies.

(b) For the classified information, the head information security officer shall establish/maintain provisions and approval procedures of security control measures for the cases that such information is processed outside of the areas requiring control measures, taking into account the risks of information leakage from the terminals and communication lines which are taken away from said areas.

(c) The head information security officer shall establish/maintain procedures for handling information using external storage media, such as USB memories.

(2) Measures to encourage information systems users to comply with the provisions

(a) Information system security officers shall examine, from perspectives of information security risks and work efficiency, the scope of support functions which encourage employees to comply with the provisions, and shall construct the information systems equipped with such functions.

(3) Basic measures for the use of information systems

(a) Employees shall not use information systems for non-work related tasks.

(b) Employees shall not connect the information systems at their own government agencies to the communication lines other than the ones so authorized by information system security officers.

(c) Employees shall not connect the information systems which are not authorized by information system security officers, to the internal communication lines at government agencies.

(d) Employees shall not use any software prohibited to use on information systems. If using unauthorized software is required to execute tasks, an approval from the information system security officer shall be granted.

(e) In such cases when an employee leaves the area where information systems are installed

and there is a risk for unauthorized operation by third parties, he or she shall implement measures to protect the systems from unauthorized use.

(f) When processing data on mobile devices which handle classified information, employees shall implement the prescribed security control measures.

(g) When removing information systems which handle confidentiality 3 information, or critical information, or vital information from the areas requiring control measures, employees shall obtain permission of the information system security officer, or the division/office information security officer.

(4) Measures when using e-mail and web

(a) When sending and receiving e-mails containing confidential information, employees shall use e-mail services provided by the servers which are operated by, or outsourced by, their own government agencies.

(b) When sending information by e-mail to the parties other than their own government agencies, employees shall use their government's domain name as the domain name of such e-mail's sender address. However, this does not apply when such employees are already known to the recipients of said e-mail.

(c) When receiving suspicious e-mails, employees shall handle them following the prescribed procedures.

(d) When it is necessary to review the web client settings, employees shall not make any setting changes which might impact on the information security.

(e) When downloading the software to the server equipment or terminals on which the web client is running, employees shall check the integrity of the software by verifying its distributor's digital signatures.

(f) When inputting and submitting the confidential information in a web form on the website they are viewing, employees shall ensure the followings.

(i) The contents to be submitted will be encrypted.

(ii) The website genuinely belongs to the organization where the contents are intended to.

(5) Handling of identification codes and user/entity authentication information

(a) Employees shall not use the information system by accessing the system through user/entity authentication with identification codes other than the ones assigned to them.

(b) Employees shall appropriately manage the identification codes assigned to them.

(c) If an employee is granted an identification code with administrator privileges, the use of such identification code shall be limited to only when they execute administrator's tasks.

(d) Employees shall manage their user/entity authentication information with utmost care.

(6) Measures for the use of encryption and digital signatures

(a) Employees shall follow the prescribed algorithms and methods when encrypting information, as well as assigning the digital signatures to the information.

(b) Employees shall follow the prescribed key management procedures, and appropriately manage the keys for decrypting the encrypted information, as well as those for assigning digital signatures to information.

(c) Employees shall take the backup of the key, following the prescribed backup procedures of the keys for decrypting the encrypted information.

(7) Prevention of malware infection

(a) Employees shall make efforts to implement measures against malware infection.

(b) In case that an employee becomes aware that an information system could have been infected by malware, he or she shall implement necessary measures, such as to immediately disconnect the infected information system from the communication lines.

8.2 Use of non-Government Furnished Terminals

8.2.1 Use of non-government furnished terminals

Purpose

Terminals provided by government agencies should be used when executing administrative tasks. However, there are situations where use of non-government furnished terminals is necessary to process information, such as while on business trips, or away from the office. If employees are not instructed to implement information security measures just because the terminals are not provided by the government agencies, the level of information security processed on such terminals could not meet the standards for measures for government agencies.

Therefore, in such cases, it is essential to preliminarily establish/maintain the security control provisions, as well as the procedures which ensure secure use of non-government furnished terminals, and have employees use such terminals under strict control of government agencies.

Even with non-government furnished terminals, information security should be maintained at the same level as that of government furnished mobile terminals. To achieve this, it is essential to refer to section 7.1.1 “Terminals” and establish/maintain provisions to ensure the same standard of security control measures, and have such measures duly implemented by employees.

Compliance Requirements

(1) Establishment/maintenance of provisions for the use of non-government furnished terminals, and management of said terminals

(a) The head information security officer shall establish/maintain procedures of granting approval and so on, when processing information on non-government furnished terminals.

(b) The head information security officer shall establish/maintain provisions related to security control measures when processing confidential information on non-government furnished terminals.

(c) Information security officers shall designate officers in charge who manage the implementation of security control measures for processing information to execute administrative tasks on non-government furnished terminals.

(d) Officers in charge who are stipulated in the preceding item shall implement measures to prevent the information theft caused by theft or loss, or malware infection, of non-government furnished terminals processing confidential information, and shall ensure employees to duly implement the security control measures.

(2) Measures for the use of non-government furnished terminals

(a) When processing information to execute administrative tasks on non-government furnished terminals, employees shall obtain an approval of the officer in charge set forth in compliance requirements 8.2.1(1) (c).

(b) When handling confidential information on non-government furnished terminals, employees shall obtain an approval of the division/office information security officer.

(c) When processing information to execute administrative tasks on non-government furnished terminals, employees shall follow the procedures and provisions related to security control measures stipulated by government agencies.

(d) Upon completion of information processing, employees shall delete the confidential information from non-government furnished terminals.